



Young People March Ltd



The Centre, City Road, March, Cambridgeshire PE15 9LS
01354 650645 Web: www.ypm.org.uk E-Mail: admin@ypm.org.uk

Online and computer safety

Acceptable use of computers and computer networks at Young People March Ltd

PURPOSE

The purpose of this policy statement, for Young People March Ltd works who work with children and young people as part of its activities. The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media, or mobile devices.
- provide staff and volunteers with the overarching principles that guide our approach to online safety.
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices. The policy statement applies to all staff, volunteers, children and young people and anyone involved in Young People March Ltd activities and members of the community.

This policy has been drawn up based on legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- bullying learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- child protection learning.nspcc.org.uk/child-protection-system

We believe that.

- children and young people should never experience abuse of any kind.
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are always kept safe. We recognise that:
 - the online world provides everyone with many opportunities; however, it can also present risks and challenges.
- we have a duty to ensure that all children, young people involved in our organisation are protected from potential harm online.
- we have a responsibility to help keep children and young people safe online, whether they are using Young People March Ltd network and devices.
 - all children, regardless of age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation, have the right to equal protection from all types of harm or abuse.
 - working in partnership with children, young people, their parents, carers, and other agencies is essential in promoting young people's welfare and in helping young people to be responsible.

We will seek to keep children and young people safe by:

- young people are always supervised,
- providing clear and specific directions to staff and volunteers on how to behave online.
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- supporting and encouraging parents and carers to do what they can to keep their children safe online.
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person reviewing and updating the security of our information systems regularly
- ensuring that usernames, logins, email accounts and passwords are used effectively.
- ensuring personal information about the children who are involved in our organisation is held securely and shared only as appropriate.
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse, and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders, and our organisation as a whole into account.
- reviewing the plan developed to address online abuse at regular intervals, to ensure that any problems have been resolved in the long term.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Child protection/safeguarding.
- Procedures for responding to concerns about a child or young person's wellbeing (safeguarding policy)
- Dealing with allegations of abuse made against a child or young person (safeguarding policy)
- Managing allegations against staff and volunteers (see safeguarding policy)
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Photography and image sharing guidance (see data protection)

This policy applies to all youth, their families and/or legal guardians, staff, volunteers,

Board Members, and members of the community.

This policy applies to all YPM computers, gaming consoles or other devices that access the internet, and YPM computer networks (including the YPM wireless network). Individuals on YPM property and/or participating in YPM activities who use their own computers, gaming consoles, smart phones, or other devices, and who access the internet through a personal wireless or cellular network are also covered by this policy.

DEFINITIONS

Acceptable Use

YPM encourages acceptable use of YPM computers, including:

- Using web browsers to obtain information from appropriate websites.
- Using e-mail for contacts.
- Using the YPM computers and/or wireless network to access outside resources that conform to this policy.
- Using the network and internet in a manner that respects the rights and property of others.
- Keeping all private accounts and passwords confidential and inaccessible to others.
- Showing responsibility by taking precautions to prevent the introduction of viruses or malicious software to the YPM computers.
- Ensuring that all attachments opened are from a known and reputable source; and, backing out of an accidentally encountered site that contains materials that violate the rules of acceptable use, and notifying a supervising staff or volunteer of the occurrence immediately.

Unacceptable Use

Users must not use the YPM computers or wireless networks in any manner that constitutes an inappropriate or unacceptable use. Examples of unacceptable use include:

- Using the internet for purposes that are illegal, unethical, or harmful to YPM.
- Engaging in cyber-bullying.
- Sending or forwarding chain or spam e-mail.
- Transmitting any content that is illegal, offensive, harassing, or fraudulent.
- Doing harm to other users' files.
- Downloading any files (including games) without prior approval of the manager.
- Interfering with, or doing harm to, the operation of the computer and/or network by installing illegal software, shareware, or freeware; and,
- Posting derogatory comments or images on social networking sites such as Facebook.

POLICY STATEMENT

The use of YPM computers and computer networks is a privilege and is subject to the terms of this policy. All persons who contravene this policy by engaging in unacceptable use of YPM

computers and/or the wireless network may lose this privilege and be subject to additional consequences.

PROCEDURES

1. When a youth, staff, volunteer, Board member, or member of the community believes that this policy has been contravened; they should notify the manager. The manager will immediately undertake an investigation of the allegations. During the investigation, the computer and computer network privileges for the individual in question may be suspended by the manager, at their discretion.
2. If the manager is directly or indirectly involved in the allegations, the matter will be directed to the Board of Directors, who will conduct the investigation.
3. Following the investigation of the allegation, the Executive Director (or Board appointed investigator, should the allegations implicate the Executive Director) shall provide a report, including a recommendation for action, to the Board of Directors within five business days of the YPM becoming aware of the allegation.
4. The Board of Directors will review the report and recommendations within five business days and take any actions deemed appropriate, which may include:
 - Loss of computer use and access to the computer network.
 - Suspension from the YPM.
 - The involvement of the police and/or other authorities or agencies.
5. The individual who raised the allegation will be notified in writing, within five days of the Board's decision, of the outcome of the investigation and any actions taken by the Board of Directors.